

# REGULAR CIRCULANT MATRICES

DANIEL APPEL

**ABSTRACT.** We consider the groups  $\text{RC}_n(\mathbb{F}_{p^t})$  and  $\text{RC}_n(\mathbb{Z}/a\mathbb{Z})$  of regular circulant  $(n \times n)$ -matrices over  $\mathbb{F}_{p^t}$  and  $\mathbb{Z}/a\mathbb{Z}$ , respectively, where  $p$  is a prime and  $t, n, a \in \mathbb{N}$ . In both cases we present a formula for the order of that group. We also make a first step towards finding the algebraic structure of these groups.

## 1. INTRODUCTION AND MAIN RESULTS

We consider regular circulant matrices over finite fields and integer residue class rings. In general, a matrix  $(a_{i,j})_{1 \leq i,j \leq n}$  is called *circulant*, if, for all  $1 \leq i, j \leq n$ , we have  $a_{i,j+1} = a_{i-1,j}$  where the indices have to be read modulo  $n$ . Hence, a circulant matrix is completely determined by any of its columns (respectively rows) and each column (respectively row) can be obtained from the previous one by a cyclic permutation.

It is commonly known that the product of two circulant matrices is again circulant and so is the inverse of a regular circulant matrix. Therefore we may consider the groups  $\text{RC}_n(\mathbb{F}_{p^t})$  and  $\text{RC}_n(\mathbb{Z}/a\mathbb{Z})$  of regular circulant  $(n \times n)$ -matrices over  $\mathbb{F}_{p^t}$  and  $\mathbb{Z}/a\mathbb{Z}$ , respectively, where  $p$  is a prime and  $t, n, a \in \mathbb{N}$ .

Let us set up some notation that we need to state our results. Suppose that  $\mathbb{F}_{p^s} \geq \mathbb{F}_{p^t}$  is a field extension. Then we write  $F^t : \mathbb{F}_{p^s} \rightarrow \mathbb{F}_{p^s}$ ,  $x \mapsto x^{p^t}$  for the relative Frobenius Homomorphism. To vectors and matrices we apply  $F^t$  componentwise. For a vector  $w = (w_i) \in \mathbb{F}_{p^s}^k$ , we define an upper triangular matrix  $T(w) := (w_{k-j+i})_{1 \leq i,j \leq k}$  where  $w_\lambda := 0$  for  $\lambda \leq 0$ . Moreover, if  $d, k \in \mathbb{N}$  with  $\gcd(d, k) = 1$ , we write  $\text{ord}_d(k)$  for the order of  $k$  in  $(\mathbb{Z}/d\mathbb{Z})^*$ . Finally, by  $\phi$  we denote the Euler function.

---

*Date:* September 18, 2009.

The author would like to thank F. Grunewald and B. Klopsch for helpful discussions. The author was supported by a Thomas Holloway Scholarship of Royal Holloway College, University of London.

**Theorem 1.1.** *Let  $p$  be a prime and  $n = mp^r \in \mathbb{N}$  with  $p \nmid m$ .*

(i) *The order of  $\text{RC}_n(\mathbb{F}_{p^t})$  is*

$$\prod_{d|m} (p^{t \cdot \text{ord}_d(p^t)} - 1)^{\phi(d)/\text{ord}_d(p^t)} \cdot p^{t \cdot (p^r - 1) \cdot \phi(d)}.$$

(ii) *Let  $\mathbb{F}_{p^s} \geq \mathbb{F}_{p^t}$  be a field extension such that  $\mathbb{F}_{p^s}$  contains the  $m$ -th roots of unity. Write the permutation  $\sigma : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ ,  $x \mapsto p^{-t}x$  as  $\sigma = \sigma_1 \cdots \sigma_l$  with disjoint cycles  $\sigma_k = (s_{k,1}, \dots, s_{k,m_k})$  of length  $m_k$ . Then, as a subgroup of  $\text{GL}_n(\mathbb{F}_{p^s})$ , the group  $\text{RC}_n(\mathbb{F}_{p^t})$  is conjugate to the group consisting of the matrices*

$$\begin{pmatrix} T(v_{(1)}) & & \\ & \ddots & \\ & & T(v_{(m)}) \end{pmatrix}$$

*with  $v_{(i)} = (v_{i,j}) \in \mathbb{F}_{p^s}^{p^r}$  satisfying*

$$v_{1,p^r}, v_{2,p^r}, \dots, v_{m,p^r} \neq 0 \text{ and}$$

$$v_{(s_{k,1})} \in \mathbb{F}_{p^{tm_k}}^{p^r}, \quad v_{(s_{k,i})} = F^{(i-1)t}(v_{(s_{k,1})})$$

*for  $2 \leq i \leq m_k$ ,  $1 \leq k \leq l$ .*

**Theorem 1.2.** *Let  $a, n \in \mathbb{N}$  and  $a = \prod_{p|a} p^{t_p}$  be the prime factorization of  $a$ . Moreover, for every prime divisor  $p$  of  $a$ , define  $r_p, m_p \in \mathbb{N}$  by  $n = p^{r_p} \cdot m_p$  with  $p \nmid m_p$ . Then the order of  $\text{RC}_n(\mathbb{Z}/a\mathbb{Z})$  is*

$$\prod_{p|a} \left( p^{n(t_p-1)} \prod_{d|m_p} (p^{\text{ord}_d(p)} - 1)^{\phi(d)/\text{ord}_d(p)} \cdot p^{(p^{r_p}-1) \cdot \phi(d)} \right).$$

We use very explicit computations to prove our results. An alternative approach would be to consider the algebra isomorphism between  $\text{RC}_n(\mathbb{F}_{p^t})$  and  $\mathbb{F}_{p^t}[x]/(x^n - 1)$ . This approach has been used to determine the number orthogonal  $(n \times n)$ -matrices over  $\mathbb{F}_{p^t}$ . See for example [2] and the references therein for further details.

From Theorem 1.1 we also obtain

**Corollary 1.3.** *Let  $p$  be a prime and  $n, t \in \mathbb{N}$ . The group  $\text{RC}_n(\mathbb{F}_{p^t}) \cap \text{SL}_n(\mathbb{F}_{p^t})$  has index  $p^t - 1$  in  $\text{RC}_n(\mathbb{F}_{p^t})$ . In particular, there are exactly  $|\text{RC}_n(\mathbb{F}_{p^t})| \cdot (p^t - 1)^{-1}$  circulant  $(n \times n)$ -matrices of determinant 1 over  $\mathbb{F}_{p^t}$*

*Proof.* We show that  $\det : \text{RC}_n(\mathbb{F}_{p^t}) \rightarrow \mathbb{F}_{p^t}^*$  is onto. Since  $\text{RC}_n(\mathbb{F}_{p^t}) \cap \text{SL}_n(\mathbb{F}_{p^t})$  is the kernel of this homomorphism, this proves the claim.

Let  $X$  be a matrix that conjugates  $\text{RC}_n(\mathbb{F}_{p^t})$  to the group given in part (ii) of Theorem 1.1. It suffices to show that  $\det : X \text{RC}_n(\mathbb{F}_{p^t}) X^{-1} \rightarrow \mathbb{F}_{p^t}^*$  is onto. Observe that  $\sigma$  has the fixed point  $m \in \mathbb{Z}/m\mathbb{Z}$ . Therefore the vector  $v_{(m)} \in \mathbb{F}_{p^t}^{p^r}$  can be chosen independently from  $v_{(1)}, \dots, v_{(m-1)}$ , subject only to the restriction that  $v_{m,p^r} \neq 0$ . Note that  $\det(T(v_{(m)})) = v_{(m,p^r)}^{p^r}$ . Since  $\gcd(p^r, p^t - 1) = 1$ , the map  $\mathbb{F}_{p^t} \rightarrow \mathbb{F}_{p^t}, x \mapsto x^{p^r}$  is a bijection. Hence, every element of  $\mathbb{F}_{p^t}^*$  can be obtained as  $\det(T(v_{(m)}))$  with suitable  $v_{(m)}$ . This implies that every element of  $\mathbb{F}_{p^t}^*$  can be obtained as the determinant of a matrix as in part (ii) of Theorem 1.1.  $\square$

## 2. PRELIMINARIES

### 2.1. Permutation induced by the Frobenius Homomorphism.

Let  $p$  be a prime and  $m, t \in \mathbb{N}$  such that  $p \nmid m$ . Moreover, let  $\mathbb{F}_{p^s} \geq \mathbb{F}_{p^t}$  be a field extension of  $\mathbb{F}_{p^t}$  that contains the  $m$ -th roots of unity and let

$$F^t : \mathbb{F}_{p^s} \longrightarrow \mathbb{F}_{p^s}, \quad x \longmapsto x^{p^t}$$

be the relative Frobenius Homomorphism. Observe that  $F^t$  induces a permutation of the  $m$ -th roots of unity, which is described by

$$(2.1) \quad \sigma : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad a \longmapsto p^t a.$$

We consider the cycle structure of this permutation. To this end, we first set up some notation.

For  $d \in \mathbb{N}$  with  $p \nmid d$  we write  $\text{ord}_d(p^t)$  for the order of  $p^t$  in  $(\mathbb{Z}/d\mathbb{Z})^*$ . By  $\langle p^t \rangle \leq (\mathbb{Z}/m\mathbb{Z})^*$  we denote the subgroup of  $(\mathbb{Z}/m\mathbb{Z})^*$  generated by  $p^t$ . Moreover, for  $d \mid m$  we set  $V_d := d \cdot \langle p^t \rangle \subseteq d \cdot (\mathbb{Z}/m\mathbb{Z})^*$ . In order to describe the permutation  $\sigma$ , we consider the action of  $\langle p^t \rangle$  on  $\mathbb{Z}/m\mathbb{Z}$  by multiplication.

Observe that

$$\mathbb{Z}/m\mathbb{Z} = \bigsqcup_{d \mid m} d \cdot (\mathbb{Z}/m\mathbb{Z})^*.$$

Moreover, each set  $d \cdot (\mathbb{Z}/m\mathbb{Z})^*$  is a disjoint union of  $|d \cdot (\mathbb{Z}/m\mathbb{Z})^*|/|V_d|$  sets of the form  $\varepsilon \cdot V_d$  with certain  $\varepsilon \in (\mathbb{Z}/m\mathbb{Z})^*$ . In particular, we have

$$\mathbb{Z}/m\mathbb{Z} = \bigsqcup_{d \mid m} \bigsqcup_{\varepsilon} \varepsilon \cdot V_d.$$

Clearly the sets  $\varepsilon \cdot V_d = \{\varepsilon d p^{tk} \mid k \in \mathbb{Z}\}$  are invariant under the action of  $\langle p^t \rangle$  and the action of  $\langle p^t \rangle$  on each set  $\varepsilon \cdot V_d$  is given by a cycle of length  $|V_d|$ . Hence, the action of  $\langle p^t \rangle$  on  $d \cdot (\mathbb{Z}/m\mathbb{Z})^*$  is described by a product of  $|d \cdot (\mathbb{Z}/m\mathbb{Z})^*|/|V_d|$  disjoint cycles of length  $|V_d|$ , that is, it has cycle structure  $(|V_d|)^{|d \cdot (\mathbb{Z}/m\mathbb{Z})^*|/|V_d|}$ . This shows that the permutation  $\sigma$  in (2.1) has cycle structure

$$\prod_{d|m} (|V_d|)^{|d \cdot (\mathbb{Z}/m\mathbb{Z})^*|/|V_d|}.$$

Now observe that for  $d \mid m$  we have  $|d \cdot (\mathbb{Z}/m\mathbb{Z})^*| = \phi(m/d)$ , where  $\phi$  denotes the Euler function. One also easily verifies that  $|V_d| = \text{ord}_{m/d}(p^t)$ . Noting that, as  $d$  runs through all divisors of  $m$ , so does  $m/d$ , we thus obtain

**Proposition 2.1.** *The permutation  $\sigma$  in (2.1) has cycle structure*

$$\prod_{d|m} (\text{ord}_d(p^t))^{\phi(d)/\text{ord}_d(p^t)}.$$

**2.2. The Kronecker Product.** Let us briefly recall the notion and some basic properties of the Kronecker product of matrices. For details we refer to [3].

Given an  $(m \times n)$ -matrix  $A = (a_{ij})$  and an  $(r \times s)$ -matrix  $B$ , the Kronecker product  $A \otimes B$  of  $A$  and  $B$  is the  $(mr \times ns)$ -matrix  $A \otimes B := (a_{ij}B)$ . By  $A^{\otimes k}$  we denote the  $k$ -fold Kronecker product of  $A$  with itself. Two standard results are

$$(A \otimes B)^{\text{tr}} = A^{\text{tr}} \otimes B^{\text{tr}} \quad \text{and} \quad (A \otimes B)^{-1} = A^{-1} \otimes B^{-1}.$$

Observe that these imply that

$$(A^{\otimes k})^{\text{tr}} = (A^{\text{tr}})^{\otimes k} \quad \text{and} \quad (A^{\otimes k})^{-1} = (A^{-1})^{\otimes k}.$$

Now let  $A, B, C, D$  all be matrices of the same dimension. Then another standard result says  $AC \otimes BD = (A \otimes B)(C \otimes D)$ . If  $A$  is regular, one easily obtains from this that

$$(ABA^{-1})^{\otimes k} = A^{\otimes k} B^{\otimes k} (A^{-1})^{\otimes k}.$$

**2.3. Pascal Matrices modulo primes.** For  $n \in \mathbb{N}$  we let  $\text{Pasc}_n(\mathbb{Z})$  be the Pascal matrix of size  $n \times n$  over  $\mathbb{Z}$ , that is,

$$\text{Pasc}_n(\mathbb{Z}) = \left( \binom{i-1}{j-1} \right)_{i,j}.$$

Let  $p$  be a prime. Then, through the natural projection  $\mathbb{Z} \rightarrow \mathbb{F}_p$ , we can also define the Pascal matrix  $\text{Pasc}_n(\mathbb{F}_p)$  over  $\mathbb{F}_p$ .

It is well known that

$$(2.2) \quad \text{Pasc}_n(\mathbb{Z})^{-1} = \left( (-1)^{i+j} \binom{i-1}{j-1} \right)_{i,j}.$$

See for example [1] for this result. As we shall see, the inverse of  $\text{Pasc}_{p^r}(\mathbb{F}_p)$ , with  $r \in \mathbb{N}$ , can also be described by a different nice formula.

**Lemma 2.2.** *Let  $p$  be a prime. Then  $\binom{p-j}{p-i} \equiv (-1)^{i+j} \binom{i-1}{j-1} \pmod{p}$  for  $1 \leq i, j \leq p$ .*

*Proof.* For  $j > i$  both terms are zero. So we may assume that  $i \geq j$ . Set  $k := i - j$  so that  $i = j + k$  and  $0 \leq k \leq p - 1$ . Observing that  $\gcd(p, k!) = 1$ , we thus find that our claim is equivalent to

$$\begin{aligned} \binom{p-j}{p-j-k} &\equiv (-1)^k \binom{j+k-1}{j-1} \pmod{p} \\ \Leftrightarrow \frac{1}{k!} \cdot \prod_{\lambda=1}^k (p-j-k+\lambda) &\equiv (-1)^k \cdot \frac{1}{k!} \cdot \prod_{\lambda=1}^k (j+k-\lambda) \pmod{p} \\ \Leftrightarrow \prod_{\lambda=1}^k (p-j-k+\lambda) &\equiv (-1)^k \prod_{\lambda=1}^k (j+k-\lambda) \pmod{p} \end{aligned}$$

which is clearly true.  $\square$

Let  $R_n$  be the  $(n \times n)$ -anti-diagonal matrix over  $\mathbb{F}_p$  with ones on the anti-diagonal. The above lemma can be rephrased as

$$\text{Pasc}_p(\mathbb{F}_p)^{-1} = \left( \binom{p-j}{p-i} \right)_{i,j} = R_p \cdot \text{Pasc}_p(\mathbb{F}_p)^{\text{tr}} \cdot R_p^{-1}.$$

In order to generalize this result to  $(p^r \times p^r)$ -matrices, we use the theorem of Lucas.

**Theorem 2.3** (Lucas' Theorem). *Let  $p$  be a prime and  $a, b \in \mathbb{N}$ . Write  $a - 1 = \sum_{i=0}^r (a_i - 1)p^i$  and  $b - 1 = \sum_{i=0}^r (b_i - 1)p^i$  with  $1 \leq a_i, b_i \leq p$ . Then*

$$\binom{a-1}{b-1} \equiv \binom{a_r-1}{b_r-1} \binom{a_{r-1}-1}{b_{r-1}-1} \cdots \binom{a_0-1}{b_0-1} \pmod{p}.$$

Let  $p, a, b, a_i, b_i$  be as in Theorem 2.3 and  $r \in \mathbb{N}$ . By definition, the  $(a, b)$  entry of  $\text{Pasc}_p(\mathbb{F}_p)^{\otimes r}$  is given by  $\binom{a_r-1}{b_r-1} \binom{a_{r-1}-1}{b_{r-1}-1} \cdots \binom{a_0-1}{b_0-1}$  which is,

by the theorem, equal to  $\binom{a-1}{b-1}$  in  $\mathbb{F}_p$ . This leads to the well known observation

$$(2.3) \quad \text{Pasc}_{p^r}(\mathbb{F}_p) = \text{Pasc}_p(\mathbb{F}_p)^{\otimes r}$$

saying that, modulo a prime, the Pascal triangle has the shape of a Sierpinski triangle.

**Corollary 2.4.** *Let  $p^r$  be a prime power. Then, over  $\mathbb{F}_p$ , we have*

$$\left( (-1)^{i+j} \cdot \binom{i-1}{j-1} \right)_{i,j} = \text{Pasc}_{p^r}(\mathbb{F}_p)^{-1} = \left( \binom{p^r-i}{p^r-j} \right)_{i,j}.$$

*Proof.* Using the above results, we find that  $\text{Pasc}_{p^r}(\mathbb{F}_p)^{-1}$  is equal to

$$\begin{aligned} (\text{Pasc}_p(\mathbb{F}_p)^{\otimes r})^{-1} &= (\text{Pasc}_{p^r}(\mathbb{F}_p)^{-1})^{\otimes r} \\ &= (R_p \cdot \text{Pasc}_p(\mathbb{F}_p)^{\text{tr}} \cdot R_p^{-1})^{\otimes r} \\ &= R_p^{\otimes r} \cdot (\text{Pasc}_p(\mathbb{F}_p)^{\text{tr}})^{\otimes r} \cdot (R_p^{-1})^{\otimes r} \\ &= R_{p^r} \cdot (\text{Pasc}_p(\mathbb{F}_p)^{\otimes r})^{\text{tr}} \cdot (R_{p^r}^{-1}). \end{aligned}$$

This implies the desired result.  $\square$

### 3. PROOFS OF THE MAIN RESULTS

**3.1. Proof of Theorem 1.1.** Let  $p$  be a prime and  $t, n \in \mathbb{N}$ . We shall always write  $n = mp^r$  with  $p \nmid m$ . Moreover, let  $\mathbb{F}_{p^s} \geq \mathbb{F}_{p^t}$  be a field extension that contains the  $m$ -th roots of unity. Consider

$$A := \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{pmatrix} \in \text{GL}_n(\mathbb{F}_{p^t}).$$

Every circulant matrix over  $\mathbb{F}_{p^t}$  can be written as  $(A^{n-1}v \ A^{n-2}v \ \cdots \ v)$  with some (unique) vector  $v \in \mathbb{F}_{p^t}^n$ . We thus want to determine the number of vectors  $v \in \mathbb{F}_{p^t}^n$  for which  $A^{n-1}v, A^{n-2}v, \dots, v$  is a basis of  $\mathbb{F}_{p^t}^n$ . Let  $X \in \text{GL}_n(\mathbb{F}_{p^t})$  and  $\tilde{A} := XAX^{-1}$ . Then we have

$$\begin{aligned} &A^{n-1}v, A^{n-2}v, \dots, v \text{ is a basis of } \mathbb{F}_{p^t}^n \\ \Leftrightarrow &XA^{n-1}v, XA^{n-2}v, \dots, Xv \text{ is a basis of } \mathbb{F}_{p^t}^n \\ \Leftrightarrow &\tilde{A}^{n-1}Xv, \tilde{A}^{n-2}Xv, \dots, Xv \text{ is a basis of } \mathbb{F}_{p^t}^n. \end{aligned}$$

Here the last equivalence holds, because  $XA^kv = XA^kX^{-1}Xv = \tilde{A}^kXv$ . Given an  $(n \times n)$ -matrix  $M$  over  $\mathbb{F}_q$ , with  $q$  a power of  $p$ , let us set

$$V(M, q) := \{v \in \mathbb{F}_q^n \mid M^{n-1}v, M^{n-2}v, \dots, v \text{ is a basis of } \mathbb{F}_q^n\}.$$

We are thus interested in the set  $V(A, p^t)$ . Observe that we have a bijection

$$V(\tilde{A}, p^s) \longrightarrow V(A, p^s), \quad v \longmapsto X^{-1}v.$$

We may therefore conjugate  $A$  into a form  $\tilde{A}$  for which  $V(\tilde{A}, p^t)$  is easier to determine. This form  $\tilde{A}$  will actually be the Jordan form of  $A$  over the field extension  $\mathbb{F}_{p^s} \geq \mathbb{F}_{p^t}$ . The above bijection also leads to a bijection

$$(3.1) \quad V(\tilde{A}, p^s) \cap X \cdot V(A, p^t) \longrightarrow V(A, p^t), \quad v \longmapsto X^{-1}v.$$

We are first going to determine the set  $V(\tilde{A}, p^s)$  and then investigate for which  $v \in V(\tilde{A}, p^s)$  we have  $X^{-1}v \in V(A, p^t)$ , that is, we then determine  $V(\tilde{A}, p^s) \cap X \cdot V(A, p^t)$ .

The characteristic polynomial  $\chi_A$  of  $A$  is given by  $\chi_A = X^n - 1$ , as one easily finds using Laplace's Theorem. Let  $\mu \in \mathbb{F}_{p^s}^*$  be a primitive  $m$ -th root of unity. Over  $\mathbb{F}_{p^s}$ , the characteristic polynomial  $\chi_A$  of  $A$  reads

$$\chi_A = X^{mp^r} - 1 = (X^m - 1)^{p^r} = \prod_{k=1}^m (X - \mu^k)^{p^r}.$$

Hence  $A$  has the eigenvalues  $\mu^k \in \mathbb{F}_{p^s}$ ,  $1 \leq k \leq m$ , each with algebraic multiplicity  $p^r$ . If  $v = (v_i)_i \in \text{Eig}(A, \mu^k)$ , we have

$$\begin{pmatrix} v_2 \\ \vdots \\ v_n \\ v_1 \end{pmatrix} = A \cdot v = \mu^k \cdot v = \begin{pmatrix} \mu^k \cdot v_1 \\ \vdots \\ \mu^k \cdot v_{n-1} \\ \mu^k \cdot v_n \end{pmatrix} \Rightarrow v = v_1 \cdot \begin{pmatrix} 1 \\ \mu^k \\ \vdots \\ \mu^{(n-1)k} \end{pmatrix}.$$

In particular,  $\text{Eig}(A, \mu^k)$  has dimension 1 and, over  $\mathbb{F}_{p^s}$ , the Jordan form  $\tilde{A}$  of  $A$  is given by

$$\tilde{A} = \begin{pmatrix} \tilde{A}_1 & & \\ & \ddots & \\ & & \tilde{A}_m \end{pmatrix} \quad \text{with} \quad \tilde{A}_b := \begin{pmatrix} \mu^b & 1 & & \\ & \mu^b & \ddots & \\ & & \ddots & 1 \\ & & & \mu^b \end{pmatrix} \in \text{GL}_{p^r}(\mathbb{F}_{p^s}).$$

In order to use (3.1), we have to determine  $X \in \text{GL}_n(\mathbb{F}_{p^s})$  such that  $XAX^{-1} = \tilde{A}$ .

For  $k \in \mathbb{N}$ , let us set

$$X(k) := \left( (-1)^{i+j} \cdot \mu^{(i-j)k} \cdot \binom{i-1}{j-1} \right) = \left( \mu^{(i-j)k} \cdot \binom{p^r-j}{p^r-i} \right) \in \text{GL}_{p^r}(\mathbb{F}_{p^s}).$$

Here the second equality follows from Corollary 2.4. We now verify that

$$X(k)^{-1} = \left( \mu^{(i-j)k} \cdot \binom{i-1}{j-1} \right).$$

To this end, note that from (2.2) we know that

$$(3.2) \quad \sum_{\lambda=1}^{p^r} (-1)^{\lambda+j} \cdot \binom{i-1}{\lambda-1} \binom{\lambda-1}{j-1} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}.$$

Hence we have

$$\begin{aligned} & \left( \mu^{(i-j)k} \cdot \binom{i-1}{j-1} \right) \cdot \left( (-1)^{i+j} \cdot \mu^{(i-j)k} \cdot \binom{i-1}{j-1} \right) \\ &= \left( \sum_{\lambda=1}^{p^r} \mu^{(i-\lambda)k} \cdot \binom{i-1}{\lambda-1} (-1)^{\lambda+j} \cdot \mu^{(\lambda-j)k} \cdot \binom{\lambda-1}{j-1} \right) \\ &= \left( \mu^{(i-j)k} \cdot \sum_{\lambda=1}^{p^r} (-1)^{\lambda+j} \cdot \binom{i-1}{\lambda-1} \binom{\lambda-1}{j-1} \right) \stackrel{(3.2)}{=} I_{p^r} \end{aligned}$$

where  $I_{p^r}$  denotes the  $(p^r \times p^r)$ -identity matrix.

Let us also set

$$Y := m^{-1} \cdot (\mu^{-ijp^r}) \in \text{GL}_m(\mathbb{F}_{p^s}).$$

We verify that the inverse of  $Y$  is given by

$$Y^{-1} = (\mu^{ijp^r}).$$

Indeed, we find

$$(\mu^{-ijp^r}) \cdot (\mu^{ijp^r}) = \left( \sum_{\lambda=1}^m \mu^{\lambda(j-i)p^r} \right) = m \cdot I_m,$$

since for  $i = j$  we have  $\mu^{\lambda(j-i)p^r} = 1$  and for  $i \neq j$  we observe that  $\mu^{(j-i)p^r}$  is a non-trivial  $m$ -th root of unity and therefore a root of the polynomial  $\sum_{\lambda=1}^m X^\lambda$ .

From the matrices  $X(k)$  and  $Y$  we construct the  $(n \times n)$ -matrix  $X$  by setting

$$X := m^{-1} \left( \mu^{-abp^r} \cdot X(a) \right)_{1 \leq a, b \leq m}.$$

Considering the above computations, one easily verifies that

$$X^{-1} = \left( \mu^{abp^r} \cdot X(b)^{-1} \right)_{a, b}.$$



We are now going to show that  $XAX^{-1} = \tilde{A}$  by considering the action of  $A$  by multiplication on the columns of  $X^{-1}$ . Let us write  $X^{-1} = (U_1 \ \cdots \ U_m)$  where for  $1 \leq b \leq m$  the  $(mp^r \times p^r)$ -submatrix  $U_b$  of  $X^{-1}$  is given by

$$U_b := \begin{pmatrix} \mu^{bp^r} \cdot X(b)^{-1} \\ \vdots \\ \mu^{abp^r} \cdot X(b)^{-1} \\ \vdots \\ X(b)^{-1} \end{pmatrix}.$$

The first column of  $\mu^{abp^r} \cdot X(b)^{-1}$  reads

$$\mu^{abp^r} \cdot \begin{pmatrix} 1 \\ \mu^b \\ \mu^{2b} \\ \vdots \\ \mu^{(p^r-1)b} \end{pmatrix} = \begin{pmatrix} \mu^{ap^rb} \\ \mu^{(ap^r+1)b} \\ \mu^{(ap^r+2)b} \\ \vdots \\ \mu^{(ap^r+(p^r-1))b} \end{pmatrix} = \begin{pmatrix} \mu^{ap^rb} \\ \mu^{(ap^r+1)b} \\ \mu^{(ap^r+2)b} \\ \vdots \\ \mu^{((a+1)p^r-1)b} \end{pmatrix}.$$

Hence the first column of  $U_b$  is given by

$$\begin{pmatrix} \mu^{p^rb} \\ \vdots \\ \mu^{(p^r+i-1)b} \\ \vdots \\ \mu^{(p^r+n-1)b} \end{pmatrix} \in \text{Eig}(A, \mu^b),$$

as desired. In general, the  $j$ -th column  $s_{a,b,j}$  of  $\mu^{abp^r} \cdot X(b)^{-1}$  reads

$$s_{a,b,j} = \mu^{abp^r} \cdot \left( \mu^{(i-j)b} \cdot \binom{i-1}{j-1} \right)_{1 \leq i \leq p^r} = \left( \mu^{(i-j+ap^r)b} \cdot \binom{i-1}{j-1} \right)_{1 \leq i \leq p^r}.$$

For  $2 \leq j \leq p^r$  we thus find

$$\begin{aligned} & \mu^b \cdot s_{a,b,j} + s_{a,b,j-1} \\ &= \mu^{abp^r+b} \cdot \left( \mu^{(i-j)b} \cdot \binom{i-1}{j-1} \right)_i + \mu^{abp^r} \cdot \left( \mu^{(i-(j-1))b} \cdot \binom{i-1}{j-2} \right)_i \\ &= \mu^{(ap^r+1)b} \cdot \left( \mu^{(i-j)b} \cdot \binom{i-1}{j-1} + \mu^{(i-j)b} \cdot \binom{i-1}{j-2} \right)_i \\ &= \mu^{(ap^r+1)b} \cdot \left( \mu^{(i-j)b} \cdot \binom{i}{j-1} \right)_i. \end{aligned}$$

Noting that, as a consequence of Lucas' Theorem,  $\binom{p^r}{j-1} = 0 = \binom{0}{j-1}$  in  $\mathbb{F}_{p^s}$  for  $2 \leq j \leq p^r$ , we write this as

$$\mu^b \cdot s_{a,b,j} + s_{a,b,j-1} = \begin{pmatrix} \mu^{(2-j+ap^r)b} \cdot \binom{1}{j-1} \\ \vdots \\ \mu^{(i+1-j+ap^r)b} \cdot \binom{i}{j-1} \\ \vdots \\ \mu^{(1-j+(a+1)p^r)b} \cdot \binom{0}{j-1} \end{pmatrix}.$$

Now let  $u_{b,j}$  be the  $j$ -th column of  $U_b$ , that is  $u_{b,j} = (s_{a,b,j})_{1 \leq a \leq m}$ . Then, for  $2 \leq j \leq p^r$ , we find

$$\mu^b \cdot u_{b,j} + u_{b,j-1} = \begin{pmatrix} \mu^b \cdot s_{1,b,j} + s_{1,b,j-1} \\ \vdots \\ \mu^b \cdot s_{a,b,j} + s_{a,b,j-1} \\ \vdots \\ \mu^b \cdot s_{m,b,j} + s_{m,b,j-1} \end{pmatrix} = \begin{pmatrix} \mu^{(2-j+p^r)b} \cdot \binom{1}{j-1} \\ \vdots \\ \mu^{(1-j+2p^r)b} \cdot \binom{0}{j-1} \\ \vdots \\ \mu^{(2-j+ap^r)b} \cdot \binom{1}{j-1} \\ \vdots \\ \mu^{(1-j+(a+1)p^r)b} \cdot \binom{0}{j-1} \\ \vdots \\ \mu^{(2+1-j+mp^r)b} \cdot \binom{1}{j-1} \\ \vdots \\ \mu^{(1-j+(m+1)p^r)b} \cdot \binom{0}{j-1} \end{pmatrix}$$

and thus  $\mu^b \cdot u_{b,j} + u_{b,j-1} = A \cdot u_{b,j}$ . This proves that  $XAX^{-1} = \tilde{A}$  indeed has the desired form.

Our next aim is to verify that

$$(3.3) \quad V(\tilde{A}, p^s) = \{(v_i)_i \in \mathbb{F}_{p^s}^n \mid v_{p^r}, v_{2p^r}, \dots, v_{mp^r} \neq 0\}.$$

To this end, we need to consider the powers  $\tilde{A}^k$  for  $1 \leq k \leq n-1$ . Obviously,  $\tilde{A}^k = \text{diag}(\tilde{A}_1^k, \dots, \tilde{A}_m^k)$ . We now show that, for  $k \in \mathbb{N}$  and  $1 \leq b \leq m$ , we have

$$\tilde{A}_b^k = \left( \mu^{(k+i-j)b} \cdot \binom{k}{j-i} \right)_{i,j}.$$

For  $\tilde{A}_b^0$  and  $\tilde{A}_b^1$  this is clear. Suppose that  $k \geq 1$  and that the claim is true for  $\tilde{A}_b^k$ . Then we have

$$\begin{aligned}
\tilde{A}_b^{k+1} &= \left( \mu^{(k+i-j)b} \cdot \binom{k}{j-i} \right)_{i,j} \cdot \left( \mu^{(1+i-j)b} \cdot \binom{1}{j-i} \right)_{i,j} \\
&= \left( \sum_{\lambda=1}^{p^r} \mu^{(k+i-\lambda)b} \cdot \binom{k}{\lambda-i} \cdot \mu^{(1+\lambda-j)b} \cdot \binom{1}{j-\lambda} \right)_{i,j} \\
&= \left( \sum_{\lambda=j-1}^j \mu^{(k+1+i-j)b} \cdot \binom{k}{\lambda-i} \cdot \binom{1}{j-\lambda} \right)_{i,j} \\
&= \left( \left( \binom{k}{j-1-i} + \binom{k}{j-i} \right) \mu^{(k+1+i-j)b} \right)_{i,j} \\
&= \left( \binom{k+1}{j-i} \mu^{(k+1+i-j)b} \right)_{i,j}
\end{aligned}$$

as claimed.

Recall that for  $w = (w_i) \in \mathbb{F}_{p^s}^{p^r}$ , we write  $T(w) = (w_{p^r-j+i})_{1 \leq i,j \leq p^r}$  where  $w_\lambda = 0$  for  $\lambda \leq 0$ . Observe that  $T(w)$  is regular, if and only if  $w_{p^r} \neq 0$ . Using the matrix  $T(w)$ , we can write

$$\begin{aligned}
\tilde{A}_b^k \cdot w &= \left( \sum_{\lambda=1}^{p^r} \mu^{(k+i-\lambda)b} \cdot \binom{k}{\lambda-i} \cdot w_\lambda \right) \\
&= \left( \sum_{\lambda=i}^{k+i} \mu^{(k+i-\lambda)b} \cdot \binom{k}{\lambda-i} \cdot w_\lambda \right) \\
&= \left( \sum_{\lambda=p^r-k}^{p^r} \mu^{(k-p^r+\lambda)b} \cdot \binom{k}{p^r-\lambda} \cdot w_{p^r-\lambda+i} \right) \\
&= \left( \sum_{\lambda=1}^{p^r} \mu^{(k-p^r+\lambda)b} \cdot \binom{k}{p^r-\lambda} \cdot w_{p^r-\lambda+i} \right) \\
&= T(w) \cdot \left( \mu^{(k-p^r+i)b} \binom{k}{p^r-i} \right).
\end{aligned}$$

We thus obtain

$$\begin{aligned}
\begin{pmatrix} \tilde{A}_b^{p^r-1} w & \tilde{A}_b^{p^r-2} w & \cdots & w \end{pmatrix} &= T(w) \cdot \left( \mu^{(p^r-j-p^r+i)b} \binom{p^r-j}{p^r-i} \right) \\
&= T(w) \cdot X(b)^{-1}.
\end{aligned}$$

We note that  $\tilde{A}_b^{kp^r} = \mu^{kbp^r} \cdot I_{p^r}$  so that  $\tilde{A}_b^{kp^r+l} = \mu^{kp^r b} \cdot \tilde{A}_b^l$ . Hence

$$\begin{aligned}
\begin{pmatrix} \tilde{A}_b^{n-1} w & \tilde{A}_b^{n-2} w & \cdots & w \end{pmatrix} &= \begin{pmatrix} \tilde{A}_b^{mp^r-1} w & \tilde{A}_b^{mp^r-2} w & \cdots & w \end{pmatrix} \\
&= T(w) \cdot \left( \mu^{(m-1)p^r b} X(b) \quad \mu^{(m-2)p^r b} X(b) \quad \cdots \quad X(b) \right).
\end{aligned}$$

Now let  $v = (v_{(i)})_{1 \leq i \leq m} \in \mathbb{F}_{p^s}^n$  where  $v_{(i)} = (v_{i,j})_{1 \leq j \leq p^r} \in \mathbb{F}_{p^s}^{p^r}$ . Then  $\tilde{A}^k v = (\tilde{A}_i^k v_{(i)})_{1 \leq i \leq m}$  so that  $\begin{pmatrix} \tilde{A}^{n-1} v & \tilde{A}^{n-2} v & \cdots & v \end{pmatrix}$  reads

$$\begin{pmatrix} \tilde{A}_1^{n-1} v_{(1)} & \tilde{A}_1^{n-2} v_{(1)} & \cdots & v_{(1)} \\ \tilde{A}_2^{n-1} v_{(2)} & \tilde{A}_2^{n-2} v_{(2)} & \cdots & v_{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{A}_m^{n-1} v_{(m)} & \tilde{A}_m^{n-2} v_{(m)} & \cdots & v_{(m)} \end{pmatrix}.$$

This can be written as the product

$$\begin{pmatrix} T(v_{(1)}) & & & \\ & T(v_{(2)}) & & \\ & & \ddots & \\ & & & T(v_{(m)}) \end{pmatrix} \cdot \begin{pmatrix} \mu^{(m-1)p^r} X(1) & \mu^{(m-2)p^r} X(1) & \cdots & X(1) \\ \mu^{2(m-1)p^r} X(2) & \mu^{2(m-2)p^r} X(2) & \cdots & X(2) \\ \vdots & \vdots & \ddots & \vdots \\ X(m) & X(m) & \cdots & X(m) \end{pmatrix}$$

where the right matrix is exactly the matrix  $m \cdot X$ . Hence

$$(3.4) \quad \begin{pmatrix} \tilde{A}^{n-1} v & \tilde{A}^{n-2} v & \cdots & v \end{pmatrix} = \text{diag}(T(v_{(1)}), \dots, T(v_{(m)})) \cdot m \cdot X.$$

Clearly, this product is regular, if and only if so are  $T(v_{(1)}), \dots, T(v_{(m)})$ , that is, if and only if  $v_{1,p^r}, \dots, v_{m,p^r} \neq 0$ . This proves (3.3).

Now we have to investigate for which  $v \in \mathbb{F}_{p^s}^n$  we have  $X^{-1}v \in \mathbb{F}_{p^t}^n$ . Recall that we write  $F^t : \mathbb{F}_{p^s} \rightarrow \mathbb{F}_{p^s}$ ,  $x \mapsto x^{p^t}$  for the relative Frobenius Homomorphism. We use the standard result that  $\mathbb{F}_{p^t} = \{x \in \mathbb{F}_{p^s} \mid F^t(x) = x\}$  to find

$$\begin{aligned} X^{-1}v \in \mathbb{F}_{p^t}^n &\Leftrightarrow F^t(X^{-1}v) = X^{-1}v \\ &\Leftrightarrow F^t(X)^{-1}F^t(v) = X^{-1}v \\ &\Leftrightarrow F^t(X)X^{-1}v = F^t(v). \end{aligned}$$

Consider the matrix  $F^t(X)X^{-1}$ . One easily sees that

$$F^t(X) = m^{-1} (\mu^{-(ap^t)bp^r} \cdot X(ap^t))$$

so that  $F^t(X) = PX$  where  $P \in \text{GL}_n(\mathbb{F}_p)$  is a permutation matrix consisting of  $(p^r \times p^r)$ -blocks which describes the permutation

$\sigma : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ ,  $a \mapsto p^{-t}a$ . Observe that the cycle structure of  $\sigma^{-1}$  and hence also of  $\sigma$  is described in Proposition 2.1. We have

$$\begin{aligned} F^t(X)X^{-1}v = F^t(v) &\Leftrightarrow Pv = F^t(v) \\ &\Leftrightarrow v_{(\sigma(i))} = F^t(v_{(i)}), \quad 1 \leq i \leq m. \end{aligned}$$

Let us write  $\sigma = \sigma_1 \cdots \sigma_l$  with disjoint cycles  $\sigma_k$  of length  $m_k$ . Clearly

$$v_{(\sigma(i))} = F^t(v_{(i)}) \quad \Leftrightarrow \quad v_{(\sigma_k(i))} = F^t(v_{(i)}), \quad 1 \leq k \leq l.$$

Writing  $\sigma_k = (s_{k,1}, \dots, s_{k,m_k})$ , the condition  $v_{(\sigma_k(i))} = F^t(v_{(i)})$ ,  $1 \leq i \leq m_k$  means

$$v_{(s_{k,i})} = F^t(v_{(s_{k,i-1})}), \quad 2 \leq i \leq m_k \text{ and } v_{(s_{k,1})} = F^t(v_{(s_{k,m_k})}).$$

By a simple substitution, we can rewrite this as

$$v_{(s_{k,i})} = F^{(i-1)t}(v_{(s_{k,1})}), \quad 2 \leq i \leq m_k \text{ and } v_{(s_{k,1})} = F^{tm_k}(v_{(s_{k,1})})$$

which in turn can be written as

$$v_{(s_{k,i})} = v_{(s_{k,1})}^{p^{(i-1)t}}, \quad 2 \leq i \leq m_k \text{ and } v_{(s_{k,1})} \in \mathbb{F}_{p^{tm_k}}^{p^r}.$$

Hence the vectors  $v = (v_{(i)}) \in V(\tilde{A}, p^s)$  for which  $X^{-1}v \in \mathbb{F}_{p^t}^n$  are precisely the ones that satisfy

$$(3.5) \quad v_{1,p^r}, v_{2,p^r}, \dots, v_{m,p^r} \neq 0,$$

$$(3.6) \quad v_{(s_{k,1})} \in \mathbb{F}_{p^{tm_k}}^{p^r}, \quad 1 \leq k \leq l,$$

$$(3.7) \quad v_{(s_{k,i})} = F^{(i-1)t}(v_{(s_{k,1})}), \quad 2 \leq i \leq m_k, \quad 1 \leq k \leq l.$$

One easily verifies that there are exactly

$$\prod_{k=1}^l (p^{tm_k} - 1)(p^{tm_k})^{p^r-1} = \prod_{k=1}^l (p^{tm_k} - 1)(p^{tm_k(p^r-1)})$$

such vectors. Using Proposition 2.1, which gives the cycle structure of  $\sigma$ , i.e. the numbers  $m_k$ , we thus obtain part(i) of Theorem 1.1.

Using our results so far, it is not difficult to prove part (ii). The group  $\text{RC}_n(\mathbb{F}_{p^t})$  consists exactly of the matrices

$$\begin{pmatrix} A^{n-1}X^{-1}v & A^{n-2}X^{-1}v & \dots & X^{-1}v \end{pmatrix}$$

with  $v \in \mathbb{F}_{p^s}^n$  satisfying (3.5), (3.6), (3.7). Observe that

$$\begin{aligned} & X \begin{pmatrix} A^{n-1}X^{-1}v & A^{n-2}X^{-1}v & \cdots & X^{-1}v \end{pmatrix} X^{-1} \\ &= \begin{pmatrix} \tilde{A}^{n-1}v & \tilde{A}^{n-2}v & \cdots & v \end{pmatrix} X^{-1} \\ &= m \cdot \text{diag}(T(v_{(1)}), \dots, T(v_{(m)})), \text{ by (3.4).} \end{aligned}$$

Since  $m \in \mathbb{F}_{p^t}^*$ , this proves part (ii) of Theorem 1.1.

**3.2. Proof of Theorem 1.2.** Let  $a, n \in \mathbb{N}$  and consider the group  $\text{RC}_n(\mathbb{Z}/a\mathbb{Z})$  of regular circulant  $(n \times n)$ -matrices over  $\mathbb{Z}/a\mathbb{Z}$ . Let  $a = p_1^{t_1} \cdots p_k^{t_k}$  be the prime factorization of  $a$ . Then the isomorphism

$$\text{GL}_n(\mathbb{Z}/a\mathbb{Z}) \xrightarrow{\cong} \text{GL}_n(\mathbb{Z}/p_1^{t_1}\mathbb{Z}) \times \cdots \times \text{GL}_n(\mathbb{Z}/p_k^{t_k}\mathbb{Z})$$

leads to an isomorphism

$$(3.8) \quad \text{RC}_n(\mathbb{Z}/a\mathbb{Z}) \xrightarrow{\cong} \text{RC}_n(\mathbb{Z}/p_1^{t_1}\mathbb{Z}) \times \cdots \times \text{RC}_n(\mathbb{Z}/p_k^{t_k}\mathbb{Z}).$$

Hence we only have to consider  $\text{RC}_n(\mathbb{Z}/p^t\mathbb{Z})$  with  $t \in \mathbb{N}$  and  $p$  prime.

We have an exact sequence

$$(3.9) \quad 1 \longrightarrow K_t \longrightarrow \text{GL}_n(\mathbb{Z}/p^{t+1}\mathbb{Z}) \longrightarrow \text{GL}_n(\mathbb{Z}/p^t\mathbb{Z}) \longrightarrow 1$$

where  $K_t = \{I_n + p^t(a_{ij}) \mid a_{ij} \in \mathbb{Z}/p^{t+1}\mathbb{Z}\}$ . Every element of  $K_t$  can be written in a unique way as  $I_n + p^t(a_{ij})$  with  $a_{ij} \in \{0, 1, \dots, p-1\}$ . Moreover,  $I_n + p^t(a_{ij})$  is circulant, if and only if  $(a_{ij})$  is. Hence we find

$$|K_t \cap \text{RC}_n(\mathbb{Z}/p^{t+1}\mathbb{Z})| = p^n.$$

Now let  $C \in \text{RC}_n(\mathbb{Z}/a\mathbb{Z})$ . We can easily lift  $C$  to  $\text{RC}_n(\mathbb{Z}/p^{t+1}\mathbb{Z})$  via the natural projection as follows. Let  $(c_i)_{1 \leq i \leq n}$  be the first column of  $C$ . For every  $c_i \in \mathbb{Z}/p^t\mathbb{Z}$ , let  $\tilde{c}_i \in \mathbb{Z}/p^{t+1}\mathbb{Z}$  be a lift and let  $\tilde{C}$  be the circulant matrix over  $\mathbb{Z}/p^{t+1}\mathbb{Z}$  with first column  $(\tilde{c}_i)$ . Obviously,  $\tilde{C}$  is a lift of  $C$ . Moreover,  $\det(\tilde{C}) \equiv \det(C) \not\equiv 0 \pmod{p}$  so that  $\det(\tilde{C})$  is a unit and  $\tilde{C}$  is regular. Hence  $\tilde{C} \in \text{RC}_n(\mathbb{Z}/p^{t+1}\mathbb{Z})$ . It follows that the sequence (3.9) leads to an exact sequence

$$1 \longrightarrow K_t \cap \text{RC}_n(\mathbb{Z}/p^{t+1}\mathbb{Z}) \longrightarrow \text{RC}_n(\mathbb{Z}/p^{t+1}\mathbb{Z}) \longrightarrow \text{RC}_n(\mathbb{Z}/p^t\mathbb{Z}) \longrightarrow 1$$

so that

$$\begin{aligned} |\text{RC}_n(\mathbb{Z}/p^{t+1}\mathbb{Z})| &= |K_t \cap \text{RC}_n(\mathbb{Z}/p^{t+1}\mathbb{Z})| \cdot |\text{RC}_n(\mathbb{Z}/p^t\mathbb{Z})| \\ &= p^n \cdot |\text{RC}_n(\mathbb{Z}/p^t\mathbb{Z})|. \end{aligned}$$

Writing  $n = p^r m$  such that  $p \nmid m$ , we know by Theorem 1.1 that

$$|\mathrm{RC}_n(\mathbb{Z}/p\mathbb{Z})| = \prod_{d|m} (p^{\mathrm{ord}_d(p)} - 1)^{\phi(d)/\mathrm{ord}_d(p)} \cdot p^{(p^r-1)\phi(d)}.$$

By induction we obtain

$$|\mathrm{RC}_n(\mathbb{Z}/p^t\mathbb{Z})| = p^{(t-1)n} \cdot \prod_{d|m} (p^{\mathrm{ord}_d(p)} - 1)^{\phi(d)/\mathrm{ord}_d(p)} \cdot p^{(p^r-1)\phi(d)}.$$

Finally, by isomorphism (3.8), this leads to Theorem 1.2.

## REFERENCES

- [1] G. CALL, D. VELLEMAN, *Pascal's matrices*. Amer. Math. Monthly **100** (1993), no. 4, 372–376.
- [2] D. JUNGnickel, T. BETH, W. GEISELMANN, *A note on orthogonal circulant matrices over finite fields*. Arch. Math. **62** (1994), 126–133.
- [3] W.-H. STEEB, *Kronecker product of matrices and applications*. BI-Wiss.-Verl., Mannheim, 1991.

DEPARTMENT OF MATHEMATICS, ROYAL HOLLOWAY COLLEGE, UNIVERSITY OF LONDON, EGHAM, SURREY, TW20 0EX, UNITED KINGDOM.

*Current address:* Mathematisches Institut der Heinrich-Heine-Universität, 40225 Düsseldorf, Germany.

*E-mail address:* Daniel.Appel@uni-duesseldorf.de